Executive Summary

Chapter 1—Introduction

The Information Assurance Technical Framework (IATF) document was developed to help a broad audience of users both define and understand their technical needs as well as to select approaches to meet those needs. The intended audience includes system security engineers, customers, scientists, researchers, product and service vendors, standards bodies, and consortia. The objectives of the IATF include raising the awareness of information assurance (IA) technologies, presenting the IA needs of information system (IS) users, providing guidance for solving IA issues, and highlighting gaps between current IA capabilities and needs. Chapter 1 outlines the information infrastructure, the information infrastructure boundaries, the IA framework areas, and general classes of threats. It then introduces the Defense-in-Depth strategy and presents the overall organization of the IATF document.

Chapter 2—Defense-in-Depth Overview

When developing an effective IA posture, all three components of the Defense-In-Depth strategy—people, technology, and operations—need to be addressed. This framework document focuses primarily on the technology aspects of Defense-in-Depth. The technology objectives and approaches explained in the sections that follow, focus on the needs of the private, public, civil, and military sectors of our society.

Chapter 2 provides an overview of the Defense-in-Depth technology objectives and gives two examples of federal computing environments. The Defense-in-Depth objectives are organized around the four Defense-in-Depth technology focus areas:

- Defend the Network and Infrastructure
  - Availability of backbone networks
  - Wireless Networks Security Framework
  - System high interconnections and virtual private networks (VPN).

- Defend the Enclave Boundary
  - Protection for network access
  - Remote access
  - Multilevel security.

- Defend the Computing Environment
  - End-user environment
  - Security for system applications.

- Supporting Infrastructures
  - Key Management Infrastructure/Public Key Infrastructure (KMI/PKI)
  - Detect and respond.

Chapter 3—Information Systems Security Engineering Process

Chapter 3 describes the systems engineering (SE) and information systems security engineering (ISSE) processes. The ISSE process is presented as a natural extension of the systems engineering process. The two processes share common elements: discovering needs, defining system functionality, designing system elements, producing and installing the system, and assessing the effectiveness of the system. Other systems processes—systems acquisition, risk management, certification and accreditation, and life-cycle support processes—are explained in relation to the ISSE process. Chapter 3 also provides suggestions on how the Common Criteria might be used to support the ISSE process. The processes described in this chapter provide the basis for the background information, technology assessments, and guidance contained in the remainder of the IATF document. An appendix, Protection Needs Elicitation (PNE), elaborates on the discover needs section of the chapter. This appendix provides a description of the process of determining or eliciting from customers their information protection needs.

Chapter 4—Technical Security Countermeasures

This chapter of the IATF provides the background for detailed technical discussions contained in later sections of the IATF. It presents a general discussion of the principles for determining appropriate technical security countermeasures. The chapter includes a detailed description of threats, including attacker motivations, information security services, and appropriate security technologies. Through use of the methodology described in Chapter 3, Information Systems Security Engineering Process, assessment of threats to the information infrastructure results in the identification of vulnerabilities followed by a managed approach to mitigating risks. Chapter 4 explains how primary security mechanisms, the robustness strategy, interoperability, and KMI/PKI should be considered in the selection of security countermeasures, technology, and mechanisms. These decisions form the basis for developing appropriate technical countermeasures for the identified threats, based on the value of the information.

Chapter 5—Defend the Network and Infrastructure

Chapter 5 describes the Defend the Network and Infrastructure technology focus area of the Defense-in-Depth strategy. The chapter describes the types of network traffic—user, control, and management—and the basic requirements to ensure that network services remain both available and secure. Organizations that operate networks should defend their networks and the infrastructures that support their networks by establishing clear service level agreements (SLA) with their commercial carriers that specify metrics for reliability, priority, and access control. Organizations must recognize that their data may be unprotected during transmission and take additional steps. Chapter 5 describes current strategies for defending networks (including data, voice, and wireless networks) and the corresponding network infrastructures.

Chapter 6—Defend the Enclave Boundary/External Connections

Defense of the enclave boundary in Chapter 6 focuses on effective control and monitoring of the data flows into and out of the enclave. Effective control measures include firewalls, guards,

VPNs, and identification and authentication (I&A)/access control for remote users. Effective monitoring mechanisms include network-based intrusion detection systems (IDS), vulnerability scanners, and virus detectors located on the local area network (LAN). These mechanisms work alone, and in concert with each other to provide defenses for those systems within the enclave. Although the primary focus of boundary protection is on protecting the inside from the outside, protected enclave boundaries also use technology and mechanisms to protect against malicious insiders who use the enclave to launch attacks or who facilitate outsider access through open doors or covert channels. The technologies discussed in Chapter 6 include firewalls, guards, virus/malicious code detection systems, IDSs, and multilevel security systems. The IA strategy for defending an enclave boundary should flexibly implement those policies governing communications between secure enclaves and between secure enclaves and external systems. The IA strategy must also provide the management capabilities for verifying compliance with policies governing defense of the enclave boundary.

Chapter 7—Defend the Computing Environment

Chapter 7 discusses the third technology focus area of the Defense-in-Depth strategy, Defend the Computing Environment. The computing environment includes the end-user workstation—both desktop and laptop—including peripheral devices. Servers include application, network, Web, file, and internal communication servers. A fundamental tenet of the Defense-in-Depth strategy is preventing cyber attacks from penetrating networks and compromising the confidentiality, integrity, and availability of the computing environment information. For those attacks that do succeed, early detection and effective response are essential to mitigating the effects of the attacks. Intrusion detection, network scanning, and host scanning are the measurement functions that, on a continuous or periodic basis, determine the effectiveness of the deployed protection systems. Chapter 7 also addresses host-based sensors, including those that operate in near real time as well as those that operate off-line.

Chapter 8—Supporting Infrastructures

Supporting Infrastructures is the fourth technology focus area of the Defense-in-Depth strategy. The IATF addresses two supporting infrastructure entities: KMI/PKI and Detect and Respond. KMI/PKI focuses on the technologies, services, and processes used to manage public key certificates and symmetric cryptography. The discussion concludes with recommendations for the features needed to achieve the three global information grid-defined assurance levels: basic, medium, and high. The Detect and Respond section of Chapter 8 addresses providing warnings, detecting and characterizing suspected cyber attacks, coordinating effective responses, and performing investigative analyses of attacks.

Chapter 9—Information Assurance for the Tactical Environment

The tactical environment, in which military or military-style operations are conducted, presents unique IA challenges. In this operational environment, there is heavy reliance on the communication of urgent, time-sensitive, or life-and-death information, often over wireless links. In the past, tactical communications equipment primarily consisted of government off-the-shelf

(GOTS) equipment. Decreased budgets and increased interoperability requirements in today's military organizations have led to the increased use of commercially developed equipment in tactical communications. Included in this use of commercial equipment is the use of commercial wireless networks and equipment in the tactical environment. Chapter 9 discusses the IA needs of the tactical environment, highlighting key tactical issues and identifying the associated security implications.

Chapter 10—A View of Aggregated Solutions

This section of the framework is included in recognition of the fact that the needs of most users are represented not by any single technology focus area, but by some combinations of them. A future release of the framework will include a discussion of developing and evaluating security approaches that are aggregations of the recommendations from the individual categories.

In Closing…

This framework document is principally intended as a reference document to provide insight and guidance to security managers and system security engineers on how to address the IA concerns of their organizations. It is tutorial (rather than prescriptive) in nature in recognition of the fact that many organizations face unique challenges that don't lend themselves to "one size fits all" solutions. This document offers insights intended to help improve the community awareness of the tradeoffs among available solutions (at a technology, not a product level) and of the desired characteristics of IA approaches for particular problems. While this framework attempts to lay out a large amount of information in an orderly sequence, it is structured to allow readers to use the table of contents to find topics of interest.